I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre o relatório final do Grupo de Contacto de Alto Nível UE-EUA sobre o intercâmbio de informações e a protecção da vida privada e dos dados pessoais

(2009/C 128/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado que institui a Comunidade Europeia, nomeadamente o artigo 286.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,

Tendo em conta o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, nomeadamente o artigo 41.º,

EMITIU O SEGUINTE PARECER

I. INTRODUÇÃO — CONTEXTO DO PARECER

1. Em 28 de Maio de 2008, a Presidência do Conselho da União Europeia anunciou ao COREPER, na perspectiva da cimeira da UE de 12 de Junho de 2008, que o Grupo de Contacto de Alto Nível UE-EUA sobre o intercâmbio de informações e a protecção da vida privada e dos dados pessoais tinha concluído o seu relatório, que foi divulgado em 26 de Junho de 2008 [1].

2. O relatório identifica princípios comuns para a protecção da vida privada e dos dados como primeiro passo para o intercâmbio de informações com os Estados Unidos com vista a lutar contra o terrorismo e a criminalidade transnacional.

3. Na sua declaração, a Presidência do Conselho anuncia que acolheria com satisfação quaisquer ideias sobre o seguimento a dar a este relatório, e nomeadamente as eventuais reacções às recomendações sobre as orientações nele preconizadas. A Autoridade Europeia para a Protecção de Dados responde a este convite emitindo o parecer a seguir apresentado, baseado na apreciação da situação tal como foi divulgada e sem prejuízo de qualquer posição que venha a tomar tendo em conta a evolução da questão.

4. A AEPD toma nota de que os trabalhos do Grupo de Contacto de Alto Nível tiveram lugar num contexto em que, em especial desde 11 de Setembro de 2001, se desenvolveu o intercâmbio de dados entre os EUA e a UE, através de acordos internacionais ou outros tipos de instrumentos. Entre estes convém referir os acordos da Europol e do Eurojust com os Estados Unidos, e igualmente os acordos PNR e o caso Swift que levaram a uma troca de cartas entre as autoridades da UE e dos EUA para estabelecer garantias de protecção mínimas dos dados [2].

[1] Documento do Conselho n.º 9831/08, disponível em: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

[2] — Acordo entre os Estados Unidos da América e o Serviço Europeu de Polícia, de 6 de Dezembro de 2001, e Acordo suplementar entre os Estados Unidos da América e o Serviço Europeu de Polícia sobre o intercâmbio de dados pessoais e informações afins, publicado no sítio interne da Europol;
— Acordo entre os Estados Unidos da América e o Eurojust sobre cooperação judicial, de 6 de Novembro de 2006, publicado no sítio interne do Eurojust;
— Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento assinado em Bruxelas em 23 Julho 2007 e em Washington em 26 Julho 2007 (Acordo PNR 2007), JO L 204/2006, de 4.8.2007, p. 18.
— Troca de cartas entre as autoridades dos EUA e da UE sobre o Programa de Detecção do Financiamento do Terrorismo, de 28 de Junho de 2007.

5. Além disso, a UE negoceia e celebra igualmente acordos semelhantes que prevêem o intercâmbio de dados pessoais com outros países terceiros. Um exemplo recente deste tipo de instrumentos é o Acordo entre a União Europeia e a Austrália sobre o tratamento de dados originários da União Europeia contidos nos Registos de Identificação dos Passageiros (PNR) e a transferência desses dados pelas transportadoras aéreas para os serviços aduaneiros da Austrália ([3]).

6. É possível constatar que o pedido de informações pessoais por parte das autoridades de aplicação da lei de países terceiros é cada vez maior, e que abrange desde bases de dados governamentais tradicionais a outros tipos de dossiês, nomeadamente dossiês de dados recolhidos pelo sector privado.

7. Enquanto elemento de referência importante, a AEPD recorda ainda que a questão da transferência de dados pessoais para países terceiros no âmbito da cooperação policial e judicial em matéria penal é tratada na Decisão-Quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal ([4]) que será provavelmente adoptada antes do final de 2008.

8. Esta troca transatlântica de informações só poderá aumentar e abranger outros sectores em que são tratados dados pessoais. Neste contexto, um diálogo sobre a «aplicação transatlântica da lei» é ao mesmo tempo bem vindo e sensível: bem vindo no sentido em que poderá proporcionar um quadro mais claro para os intercâmbios de dados actuais ou futuros; sensível porque esse quadro poderá legitimar transferências maciças de dados num domínio — aplicação da lei — em que o impacto sobre os indivíduos é particularmente grave, e em que são ainda mais necessárias salvaguardar e garantias rigorosas e fiáveis ([5]).

9. O presente parecer tratará no capítulo seguinte da situação actual e dos possíveis rumos a tomar. O Capítulo III incidirá no âmbito e natureza de um instrumento que permita a partilha da informação. No Capítulo IV, o parecer analisará de uma perspectiva jurídica geral as questões ligadas ao conteúdo de um eventual acordo. Tratará de questões como as condições de avaliação do nível de protecção previsto pelos Estados Unidos, e discutirá a questão da utilização do quadro regulador da UE como marco de referência, a fim de avaliar o nível de protecção. Este capítulo conterá igualmente uma lista das exigências de base a incluir neste tipo de acordo. Por último, no Capítulo V, o presente parecer fornecerá uma análise dos princípios de privacidade que se prendem com o conteúdo do relatório.

([3]) JO L 213 de 8.8.2008, p. 49.

([4]) Decisão-Quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, versão de 24 de Junho de 2008 disponível em http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Quanto à necessidade de um quadro jurídico claro, ver Capítulos III e IV do presente parecer.

II. SITUAÇÃO ACTUAL E POSSÍVEIS RUMOS A TOMAR

10. A AEPD avalia a situação actual do seguinte modo: foram realizados alguns progressos no que diz respeito à definição de normas comuns relativas ao intercâmbio de informação e à protecção da vida privada e dos dados pessoais.

11. No entanto, os trabalhos preparatórios para qualquer tipo de acordo entre a UE e os EUA não estão ainda concluídos, sendo necessário prosseguir os trabalhos. O relatório do Grupo de Contacto de Alto Nível refere uma série de questões pendentes das quais a questão preponderante é a questão da «reparação». Persiste o desacordo sobre o âmbito necessário da reparação judicial ([6]). Foram identificadas outras cinco questões pendentes no Capítulo 3 do relatório. Além disso, decorre do presente parecer que muitas outras questões ainda não estão resolvidas, como por exemplo as respeitantes ao âmbito e natureza de um instrumento relativo ao intercâmbio da informação.

12. Uma vez que a opção preferida no relatório é um acordo vinculativo — preferência partilhada pela AEPD — é ainda mais necessário usar de prudência. Antes de se poder chegar a um acordo, é necessário um trabalho de preparação cuidadoso e aprofundado.

13. Por último, de acordo com a AEPD, o âmbito mais indicado para a celebração de um acordo seria o Tratado de Lisboa, na condição, obviamente, de que este entre em vigor. Com efeito, ao abrigo do Tratado de Lisboa, não se poria a questão da incerteza jurídica sobre a linha divisória entre os pilares da UE. Além disso, seria garantido o total envolvimento do Parlamento Europeu bem como o controlo judicial do Tribunal de Justiça.

14. Nessas circunstâncias, a melhor maneira de avançar seria elaborar um roteiro com vista a um eventual acordo numa fase posterior. Esse roteiro incluiria os seguintes elementos:

— Orientações para o prosseguimento dos trabalhos do Grupo de Contacto de Alto Nível (ou de qualquer outro grupo) bem como um calendário;

— Numa fase inicial, discussão e possível acordo sobre questões fundamentais como o âmbito e a natureza do acordo;

— Com base num entendimento comum destas questões fundamentais, o aprofundamento dos princípios relativos à protecção dos dados;

— Participação das partes interessadas nas diferentes fases do processo;

— Do lado europeu, tratamento das restrições institucionais.

([6]) Página 5 do relatório, parte C.

III. **ÂMBITO E NATUREZA DE UM INSTRUMENTO RELATIVO À PARTILHA DA INFORMAÇÃO**

15. No entender da AEPD, é essencial que o âmbito e a natureza de um eventual instrumento que inclua princípios de protecção dos dados sejam claramente definidos, enquanto primeiro passo para o desenvolvimento de tal instrumento.

16. Quanto ao âmbito, as questões importantes que exigem resposta são:

— quais são os actores envolvidos, dentro e fora da área de aplicação da lei;

— o que se pretende com o «objectivo de aplicação da lei» e a sua relação com outros objectivos como a segurança nacional, e mais especificamente o controlo das fronteiras e a saúde pública;

— de que maneira este instrumento se pode inserir na perspectiva de uma zona de segurança transatlântica global.

17. A definição da natureza deverá clarificar as seguintes questões:

— se tal for pertinente, ao abrigo de que pilar o instrumento será negociado;

— se o instrumento em questão será vinculativo para a UE e os EUA;

— se o mesmo terá efeitos directos, no sentido em que prevê direitos e obrigações para as pessoas que podem ser aplicados junto de uma autoridade judicial;

— se o instrumento em si permitirá o intercâmbio de informação ou estabelecerá uma norma mínima para o intercâmbio de informação a complementar através de acordos específicos;

— de que modo o instrumento se articulará com os instrumentos existentes: respeitá-los-á, substitui-los-á ou complementá-los-á?

III.1. **Escolha do instrumento**

Actores envolvidos

18. Embora não haja uma indicação clara no relatório do Grupo de Contacto de Alto Nível sobre o âmbito exacto do futuro instrumento, pode ser deduzido dos princípios nele referidos que prevê abranger tanto as transferências entre intervenientes públicos e privados ([7]) como entre as autoridades públicas.

([7]) Ver em especial o Capítulo 3 do relatório, «Questões pendentes pertinentes para as relações transatlânticas», ponto 1: «Coerência das obrigações das entidades privadas durante as transferências de dados».

— Entre os intervenientes públicos e privados:

19. A AEPD reconhece a lógica da aplicabilidade de um futuro instrumento às transferências entre actores públicos e privados. O desenvolvimento de tal instrumento é realizado na sequência dos pedidos apresentados pela parte EUA de informação provenientes de partes privadas nos últimos anos. A AEPD toma nota de que os actores privados estão a tornar-se uma fonte de informação sistemática numa perspectiva de aplicação da lei, seja a nível dos EUA, seja a nível internacional ([8]). O caso SWIFT constituiu um precedente importante, tendo uma empresa privada sido solicitada a transmitir sistematicamente os dados em grande quantidade às autoridades de aplicação da lei de um Estado terceiro ([9]). A recolha de dados PNR das companhias de aviação insere-se na mesma lógica. No seu parecer sobre um projecto de decisão-quadro para um sistema europeu de PNR, a AEPD já questionou a legitimidade desta tendência ([10]).

20. Há mais duas razões para estar relutante quanto à inclusão de transferências entre intervenientes públicos e privados no âmbito de um futuro instrumento.

21. Em primeiro lugar, tal inclusão poderá ter um efeito não desejado no território da própria UE. A AEPD está seriamente preocupada com a possibilidade de empresas privadas (tais como instituições financeiras) serem, em princípio, transferidas para países terceiros, uma vez que tal poderia provocar uma forte pressão no sentido de disponibilizar igualmente na UE o mesmo tipo de dados às autoridades de aplicação da lei. O sistema PNR é um exemplo de um desenvolvimento não desejado desse tipo, que teve início com uma recolha em larga escala de dados relativos aos passageiros nos EUA, que foram seguidamente transpostos para o contexto interno europeu ([11]) sem que a necessidade e a proporcionalidade do sistema tenham sido claramente demonstradas.

22. Em segundo lugar, no seu parecer sobre a proposta da Comissão relativa aos dados PNR da UE a AEPD levantou igualmente a questão do âmbito de protecção dos dados (primeiro ou terceiro pilar) aplicável às condições da

([8]) Ver sobre esta questão o parecer da AEDP de 20 de Dezembro de 2007 sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* — PNR) para efeitos de aplicação da lei, JO C 110 de 1.5.2008, p. 1. «Tradicionalmente, tem havido uma clara separação entre as actividades policiais e as do sector privado, sendo as funções policiais desempenhadas por serviços especificamente dedicados, em particular as forças de polícia, e sendo os intervenientes privados solicitados, caso a caso, a comunicar dados pessoais a esses serviços de aplicação da lei. Há agora uma tendência para impor a cooperação para efeitos de aplicação da lei a intervenientes privados numa base sistemática».

([9]) Ver parecer 10/2006, de 22 de Novembro de 2006, do Grupo do Artigo 29. sobre o tratamento de dados pessoais pela Sociedade Mundial de Telecomunicações Financeiras Interbancárias (SWIFT), WP 128.

([10]) Parecer emitido em 20 de Dezembro de 2007.

([11]) Ver a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* — PNR) para efeitos de aplicação da lei, referida na nota de pé-de-página 8, tal como actualmente debatida no Conselho.

cooperação entre os intervenientes públicos e privados: deverão as regras ser baseadas na qualidade do controlador de dados (sector privado) ou na finalidade prosseguida (aplicação da lei)? A linha de demarcação entre o primeiro e o terceiro pilar está longe de ser clara em situações em que são impostas obrigações aos intervenientes privados de tratar os dados pessoais para efeitos de aplicação da lei. Neste contexto é digno de nota que o Advogado-Geral Yves Bot, no seu recente parecer no processo relativo à conservação de dados ([12]) proponha uma linha de demarcação para estas situações, mas acrescenta à sua proposta: «Esta linha de demarcação não está com certeza isenta de críticas e pode, sob determinados aspectos, parecer superficial.» A AEPD toma nota igualmente de que o acórdão PNR do Tribunal ([13]) não dá resposta cabal à questão do quadro jurídico aplicável. Por exemplo, o facto de certas actividades não estarem abrangidas pela Directiva 95/46/CE não significa automaticamente que essas actividades podem ser reguladas ao abrigo do terceiro pilar. O referido acórdão resulta possivelmente numa lacuna no que diz respeito à legislação aplicável e em todo o caso gera incerteza jurídica no que se refere às garantias jurídicas disponíveis para as pessoas em causa.

23. Nesta perspectiva, a AEPD salienta que deverá ser garantido que um futuro instrumento que preveja princípios gerais de protecção de dados não pode legitimar as transferências transatlânticas de dados pessoais entre intervenientes públicos e privados. Estas transferências apenas podem ser incluídas num futuro instrumento desde que:

— o futuro instrumento estipule que a transferência só é autorizada se se comprovar que é absolutamente necessária para um fim específico, a decidir caso a caso,

— a própria transferência for rodeada por importantes garantias de protecção dos dados (tal como descrito no presente parecer).

Além disso, a AEPD toma nota da incerteza quanto ao quadro de protecção de dados aplicável e argumenta, portanto, em todo o caso a favor da não inclusão das transferências de dados pessoais entre entidades públicas e privadas no estado actual da legislação da UE.

— Entre autoridades públicas:

24. O âmbito exacto do intercâmbio de informação não é claro. Como primeiro passo no prosseguimento dos trabalhos com vista à criação de um instrumento comum, o âmbito previsto para tal instrumento deverá ser clarificado. Subsistem designadamente algumas questões:

— No que diz respeito às bases de dados situadas na UE, o instrumento em causa visará as bases de dados centralizadas (parcialmente) geridas pela UE como as bases de dados da Europol e do Eurojust, ou as bases de dados descentralizadas geridas pelos Estados-Membros, ou tanto umas como outras?

— O âmbito do instrumento alarga-se às redes interconexas, ou seja, as garantias previstas abrangerão os dados intercambiados entre os Estados-Membros ou as agências, na UE bem como nos EUA?

— O instrumento abrangerá apenas o intercâmbio entre bases de dados no domínio da aplicação da lei (polícia, justiça, eventualmente as alfândegas) ou igualmente outras bases de dados como as bases de dados fiscais?

— O instrumento também abrangerá as bases de dados de agências nacionais de segurança, ou permitirá o acesso por essas agências a bases de dados das autoridades de aplicação da lei no território da outra parte contratante (EUA à UE e vice-versa)?

— O instrumento abrangerá as transferências de informação caso a caso, ou o acesso permanente às bases de dados existentes? Esta última hipótese levantará certamente questões relativas à proporcionalidade, tal como exposto de forma mais aprofundada no ponto 3 do Capítulo V.

Objectivo da aplicação da lei

25. A definição do objectivo de um eventual acordo também suscita incerteza. O objectivo da aplicação da lei é claramente indicado na introdução bem como no primeiro princípio anexo ao relatório, e será analisado em profundidade no Capítulo IV do presente parecer. A AEPD toma nota de que decorre do atrás exposto que o intercâmbio de dados incidirá em questões do terceiro pilar, mas poder-se-á pôr a questão de saber se se trata apenas de um primeiro passo no sentido de uma troca de informação mais ampla. Parece claro que objectivo da «segurança pública» exposto no relatório inclui a luta contra o terrorismo, a criminalidade organizada e outros crimes. No entanto, será que também permite o intercâmbio de dados no caso de outros interesses públicos como eventuais riscos de saúde pública?

26. A AEPD recomenda que o objectivo seja restringido ao tratamento de dados identificados com precisão e à justificação das escolhas de política conducentes a essa definição do objectivo.

([12]) Parecer do Advogado-Geral Yves Bot de 14 de Outubro de 2008, Irlanda c/Parlamento Europeu e Conselho (Processo C-301/06), ponto 108.

([13]) Decisão do Tribunal de 30 de Maio de 2006, Parlamento Europeu c/Conselho da União Europeia (C-317/04) e Comissão Europeia (C-318/04), Processos apensos C-317/04 e C-318/04, Col. [2006], p. I-4721.

Um espaço transatlântico de segurança global

27. O vasto âmbito deste relatório deverá ser colocado na perspectiva da zona de segurança transatlântica global discutida pelo chamado «Grupo do Futuro» ([14]). O relatório deste Grupo, apresentado em Junho de 2008, põe um certo ênfase na dimensão externa da política de assuntos internos e advoga que «*até 2014, a União Europeia deverá ter tomado posição quanto ao objectivo político de realizar com os Estados Unidos um espaço euro-atlântico de cooperação no domínio da liberdade, segurança e justiça*». Tal cooperação iria além da segurança em sentido estrito e incluiria temas tratados no actual Título IV do Tratado CE, como a imigração, os vistos e o asilo e a cooperação no domínio do direito civil. Importa levantar a questão de saber até que ponto um acordo relativo a princípios de protecção de base, como os referidos no relatório do Grupo de Contacto de Alto Nível, poderá e deverá constituir a base para um intercâmbio de informação numa área tão vasta.

28. Normalmente, até 2014 a estrutura de pilares deixará de existir e não haverá uma base jurídica para a protecção de dados dentro da própria UE (ao abrigo do Tratado de Lisboa, artigo 16.º do Tratado relativo ao funcionamento da União Europeia). No entanto, o facto de haver harmonização a nível da UE no que diz respeito à *regulamentação* da protecção de dados não implica que qualquer acordo com um país terceiro possa prever a *transferência* de quaisquer dados pessoais, qualquer que seja o seu objectivo. Consoante o contexto e as condições do tratamento, poderão ser exigidas garantias de protecção de dados adequadas para domínios específicos como a aplicação da lei. A AEPD recomenda que sejam tidas em conta as consequências destas diferentes perspectivas na elaboração de um futuro acordo.

III.2. **Natureza do acordo**

O quadro institucional europeu

29. Numa perspectiva a curto prazo, em todo o caso, é essencial determinar ao abrigo de que pilar o acordo será negociado. Tal é necessário nomeadamente dado que o quadro regulador interno para a protecção de dados será afectado por tal acordo. O quadro será o do primeiro pilar — basicamente a Directiva 95/46/CE com o seu regime específico para a transferência de dados para países terceiros — ou o do terceiro pilar com um regime menos restritivo aplicável às transferências para países terceiros? ([15]).

30. Embora o objectivo da aplicação da lei prevaleça, tal como já referido, o relatório do Grupo de Contacto de Alto Nível refere no entanto a recolha de dados junto de intervenientes privados, e os objectivos podem igualmente ser interpretados em sentido lato susceptível de ir além da segurança, incluindo por exemplo as questões relativas à imigração e ao controlo das fronteiras, mas também possivelmente à saúde pública. Face a estas incertezas, seria francamente preferível esperar pela harmonização dos pilares ao abrigo da legislação da UE, tal como previsto no Tratado de Lisboa, para estabelecer claramente a base jurídica para as negociações e o papel exacto das instituições europeias, especialmente o do Parlamento Europeu e da Comissão.

Carácter vinculativo do instrumento

31. Deverá ficar claro se as conclusões dos debates resultarão num memorando de entendimento ou noutro instrumento não vinculativo, ou num acordo internacional vinculativo.

32. A AEPD apoia a preferência dada no relatório a um acordo vinculativo. Um acordo oficial vinculativo é, no entender da AEPD, uma condição prévia indispensável a qualquer transferência para fora da UE, independentemente do respectivo objectivo. Não é possível efectuar nenhuma transferência de dados para um país terceiro sem que as condições e garantias adequadas estejam previstas num quadro jurídico específico (e vinculativo). Por outras palavras, um memorando de entendimento ou outro instrumento não vinculativo pode ser útil para proporcionar orientação para as negociações de outros instrumentos vinculativos, mas não pode nunca sobrepor-se à necessidade de um acordo vinculativo.

Efeito directo

33. As disposições do instrumento deverão ser igualmente vinculativas para os EUA e para a UE e seus Estados-Membros.

34. Deverá além disso ser garantido que as pessoas têm direito a exercer os seus direitos e nomeadamente a obter reparação, com base nos princípios acordados. De acordo com a AEPD, a melhor maneira de o conseguir é formular as disposições substantivas do instrumento de forma a que estas produzam efeito directo para os residentes da União Europeia e possam ser invocadas em tribunal. O efeito directo das disposições de um acordo internacional, bem como as condições da sua transposição para a legislação europeia e nacional destinadas a garantir a eficácia das medidas têm de ser clarificados no instrumento.

Relações com outros instrumentos

35. Em que medida o acordo é autónomo ou tem de ser completado caso a caso por outros acordos sobre intercâmbios específicos de dados constitui igualmente uma questão fundamental. Põe-se, de facto, a questão de saber se um simples acordo poderá abranger de forma adequada, com um conjunto de normas único, as múltiplas

([14]) Relatório do Grupo Consultivo Informal de Alto Nível sobre o Futuro da Política Europeia de Assuntos Internos, «Liberdade, Segurança, Vida Privada — Política Europeia de Assuntos Internos num mundo aberto», Junho de 2008, disponível em register.consilium.europa.eu

([15]) Ver artigos 11.º a 13.º da Decisão-Quadro relativa à protecção de dados pessoais referida no ponto 7 do presente parecer.

especificidades do tratamento de dados no terceiro pilar. Ainda suscita mais dúvidas que o referido acordo possa *permitir*, sem debate e garantias adicionais, uma aprovação global de qualquer transferência de dados pessoais qualquer que seja o seu objectivo e natureza. Além disso, os acordos com países terceiros não são necessariamente permanentes, uma vez que podem ser ligados a ameaças específicas, ser sujeitos a revisão e a cláusulas de caducidade. Por outro lado, as normas mínimas comuns tal como reconhecidas num instrumento vinculativo poderão facilitar os debates sobre a transferência de dados pessoais em relação com uma base de dados concreta ou operações de tratamento de dados.

36. A AEPD seria, portanto, favorável ao desenvolvimento de um conjunto mínimo de critérios de protecção de dados a complementar caso a caso através de disposições adicionais específicas, tal como referido no relatório do Grupo de Contacto de Alto Nível, em vez da alternativa de um acordo autónomo. Estas disposições específicas adicionais são uma condição prévia para permitir a transferência de dados num caso específico. Tal constituiria um incentivo a uma abordagem harmonizada em termos de protecção de dados.

Aplicação aos instrumentos existentes

37. Deverá igualmente analisar-se de que forma um eventual acordo geral se articularia com os acordos já existentes celebrados entre a UE e os EUA. Convém notar que estes acordos não têm o mesmo carácter vinculativo: merecem referência especial o acordo PNR (o que apresenta o maior grau de certeza jurídica), os acordos Europol e Eurojust, ou a troca de cartas SWIFT ([16]). Será que um novo quadro geral viria complementar estes instrumentos existentes ou estes se manteriam inalterados, uma vez que o novo quadro seria aplicável apenas a outros intercâmbios futuros de dados pessoais? No entender da AEPD, a coerência jurídica exigiria um conjunto de regras harmonizado que seja aplicável tanto aos acordos existentes como aos acordos futuros em matéria de transferências de dados e que os complemente.

38. A aplicação do acordo geral aos instrumentos existentes teria a vantagem de reforçar o carácter vinculativo destes. Tal seria particularmente apreciado no que diz respeito aos instrumentos que não são juridicamente vinculativos, como a troca de cartas SWIFT, uma vez que imporia o cumprimento de um conjunto de princípios gerais relativos à vida privada.

IV. **AVALIAÇÃO JURÍDICA GERAL**

39. Este capítulo analisará a forma de avaliar o nível de protecção de um quadro ou instrumento específico, incluindo a questão dos marcos de referência a utilizar e as exigências de base necessários.

Nível de protecção adequado

40. De acordo com a AEPD, deverá ser claro que um dos principais resultados de um futuro instrumento será que a transferência de dados pessoais para os Estados Unidos só se poderá efectuar desde que as autoridades dos Estados Unidos garantam um nível de protecção adequado (e vice-versa).

41. A AEPD considera que só um verdadeiro teste de adequação dá garantias suficientes no que diz respeito ao nível de protecção dos dados pessoais. Considera que um acordo-quadro geral com um âmbito tão vasto como o preconizado no relatório do Grupo de Contacto de Alto Nível teria dificuldades em passar, enquanto tal, um verdadeiro teste de adequação. A adequação do acordo geral apenas poderá ser reconhecida se for combinada com a adequação dos acordos específicos celebrados caso a caso.

42. A apreciação do nível de protecção oferecido pelos países terceiros não é um exercício inabitual, em especial para a Comissão Europeia: a adequação é, ao abrigo do primeiro pilar, uma exigência para a transferência. Foi avaliada em diversas ocasiões nos termos do artigo 25.º da Directiva 95/46 com base em critérios específicos e confirmada por decisões da Comissão Europeia ([17]). Ao abrigo do terceiro pilar, tal sistema não é explicitamente previsto: a avaliação da adequação da protecção apenas é recomendada na situação específica dos artigos 11.º e 13.º da (ainda não adoptada) decisão-quadro relativa à protecção dos dados ([18]) e é deixada aos Estados-Membros.

43. No caso em apreço, o âmbito do exercício abrange o objectivo da aplicação da lei, sendo os debates conduzidos pela Comissão sob supervisão do Conselho. O contexto é diferente da avaliação dos princípios de «porto seguro» ou a adequação da legislação canadiana, e tem mais ligações com as recentes negociações PNR com os EUA e a Austrália que se desenrolaram num quadro jurídico do terceiro pilar. No entanto, os princípios do Grupo de Contacto de Alto Nível foram igualmente mencionados no contexto do programa de isenção de vistos que diz respeito às fronteiras e à imigração e portanto às questões do primeiro pilar.

44. A AEPD recomenda que qualquer averiguação da adequação ao abrigo de um futuro instrumento deverá basear-se

([16]) Ver nota de pé-de-página 2.

([17]) As decisões da Comissão sobre a adequação da protecção dos dados pessoais nos países terceiros, incluindo a Argentina, o Canadá, a Suíça, os Estados Unidos, Guernsey, a Ilha de Man e Jersey estão disponíveis em http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Restringida à transferência por um Estado-Membro para um país terceiro ou organismo internacional de dados recebidos de uma autoridade competente de outro Estado-Membro.

nas experiências adquiridas nestes diferentes domínios. Recomenda que a noção de «adequação» no contexto de um futuro instrumento seja desenvolvida com base em critérios semelhantes aos utilizados em anteriores avaliações da adequação.

Reconhecimento mútuo — reciprocidade

45. Um segundo elemento do nível de protecção diz respeito ao reconhecimento mútuo pela UE e pelos EUA dos respectivos sistemas. O relatório do Grupo de Contacto de Alto Nível refere a este respeito que o objectivo seria obter o reconhecimento da eficácia dos respectivos sistemas de protecção da vida privada e dos dados nos domínios abrangidos por estes princípios ([19]) e chegar a uma aplicação equivalente e recíproca da legislação relativa à protecção da vida privada e dos dados pessoais.

46. Para a AEPD é óbvio que o reconhecimento mútuo (ou reciprocidade) apenas é possível se for garantido um nível de protecção adequado. Por outras palavras, o futuro instrumento deverá harmonizar um nível mínimo de protecção (através de uma averiguação da adequação, tendo em conta a necessidade de acordos específicos numa base caso a caso). Só com base nesta condição prévia poderá ser reconhecida a reciprocidade.

47. O primeiro elemento a ter em conta é a reciprocidade das disposições substantivas em matéria de protecção de dados. Na opinião da AEPD, um acordo deveria abranger o conceito de reciprocidade das disposições substantivas em matéria de protecção de dados por forma a garantir, por um lado, que o tratamento dos dados no território da UE (e dos EUA) respeite plenamente a legislação nacional relativa à protecção de dados, e, por outro, que o tratamento dos dados fora do respectivo país de origem e abrangido pelo acordo respeite os princípios da protecção de dados tal como constam do acordo.

48. O segundo elemento é a reciprocidade dos mecanismos de reparação. Dever-se-ia garantir que os cidadãos europeus disponham de vias de recurso adequadas quando os dados que lhes dizem respeito sejam tratados nos Estados Unidos (independentemente da legislação aplicável a esse tratamento), mas igualmente que a União Europeia e os seus Estados-Membros concedam direitos equivalentes aos cidadãos dos EUA.

49. O terceiro elemento é a reciprocidade do acesso aos dados pessoais pelas autoridades de aplicação da lei. Se um instrumento permite às autoridades dos Estados Unidos o acesso a dados provenientes da União Europeia, a reciprocidade implica que seja concedido às autoridades da UE igual acesso a dados provenientes dos EUA. A reciprocidade não deve afectar a eficácia da protecção da pessoa em causa. Esta é uma condição prévia para permitir o acesso «transatlântico» pelas autoridades de aplicação da lei. Isto significa, concretamente, que:

— Não deve ser permitido o acesso directo pelas autoridades dos Estados Unidos a dados dentro do território da UE (e vice-versa). O acesso apenas deverá ser concedido numa base indirecta no âmbito de um sistema de «empurro»;

— Esse acesso deverá efectuar-se sob o controlo das autoridades responsáveis pela protecção dos dados e das autoridades judiciais do país em que ocorre o tratamento dos dados;

— O acesso das autoridades dos Estados Unidos às bases de dados na UE deverá respeitar as disposições substantivas em matéria de protecção de dados (ver atrás) e garantir uma reparação total à pessoa em causa.

Precisão do instrumento

50. A especificação das condições de avaliação (adequação, equivalência, reconhecimento mútuo) é essencial uma vez que determina o conteúdo, em termos de precisão, certeza jurídica e eficácia da protecção. O conteúdo de um futuro instrumento tem de ser preciso e exacto.

51. Além disso, deverá ficar claro que qualquer acordo específico celebrado posteriormente terá de incluir garantias de protecção de dados pormenorizadas e completas sobre a pessoa concernida pelo intercâmbio de dados previsto. Só um nível duplo deste tipo de princípios concretos de protecção de dados garantirá a necessária harmonização entre o acordo geral e os acordos específicos, tal como já observado nos pontos 35 e 36 do presente parecer.

Desenvolver um modelo para outros países terceiros

52. Merece especial atenção a questão de saber até que ponto um acordo com os EUA poderá ser um modelo para outros países terceiros. A AEPD toma nota de que, além dos EUA, o referido relatório do Grupo do Futuro também indica a Rússia como parceiro estratégico da UE. Na medida em que os princípios são neutros e respeitam as garantias fundamentais da UE, poderão constituir um precedente útil. No entanto, eventuais especificidades ligadas, por ex, ao quadro jurídico do país destinatário ou ao objectivo da transferência poderão impedir a mera transposição do acordo. Outro factor igualmente decisivo será a situação dos países terceiros em termos de democracia: dever-se-á assegurar que os princípios acordados serão efectivamente garantidos e implementados no país destinatário.

Que marcos de referência para avaliar o nível de protecção?

53. A adequação, implícita ou explícita, deverá respeitar o quadro jurídico internacional e europeu e sobretudo, as garantias de protecção de dados acordadas em comum, as quais estão consagradas nas Orientações das Nações Unidas,

([19]) Capítulo A. Acordo internacional vinculativo, p. 8.

na Convenção 108 do Conselho da Europa e o seu protocolo adicional, nas Orientações da OCDE e no projecto de decisão-quadro relativa à protecção dos dados, bem como, para os aspectos do primeiro pilar, na Directiva 95/46/CE ([20]). Todos estes instrumentos contêm princípios semelhantes que são mais amplamente reconhecidos como sendo a parte essencial da protecção de dados pessoais.

54. É muito importante que os princípios atrás referidos sejam devidamente tidos em conta, se se atender ao impacto de um potencial acordo como o previsto no relatório do Grupo de Contacto de Alto Nível. Um instrumento que abranja todo o sector de *aplicação da lei* de um país terceiro constituiria de facto uma situação sem precedente. As decisões sobre a adequação existentes no primeiro pilar, bem como os acordos celebrados com países terceiros no terceiro pilar da UE (Europol, Eurojust) estiveram sempre ligados a uma transferência de dados específica, enquanto neste caso poderiam ser tornadas possíveis transferências com um âmbito muito mais vasto, tendo em conta o grande objectivo prosseguido (combate às infracções penais, segurança pública e nacional, controlo das fronteiras) e o número desconhecido de bases de dados abrangidas.

Exigências de base

55. As condições a preencher no contexto da transferência de dados pessoais para países terceiros foram elaboradas num documento de trabalho do Grupo do Artigo 29.º ([21]). Qualquer acordo sobre princípios relativos à vida privada deverá ser sujeito a um teste de conformidade que garanta a eficácia das garantias de protecção dos dados.

— Quanto ao fundo: os princípios relativos à protecção dos dados deverão prever um alto nível de protecção, e cumprir normas que estejam em consonância com os princípios da UE. Os 12 princípios incluídos no relatório do Grupo de Contacto de Alto Nível continuarão a ser analisados na perspectiva do Capítulo V do presente parecer;

— Quanto à concretização: dependendo da natureza do acordo, e em especial no caso de se tratar de um acordo oficial internacional, as regras e procedimentos deverão ser definidos em pormenor, por forma a permitir uma execução efectiva;

— Quanto à supervisão: a fim de garantir o cumprimento das regras acordadas, deverão ser instituídos mecanismos de controlo, tanto a nível interno (auditorias) como externo (revisões). Esses mecanismos têm de ser igualmente acessíveis a ambas as partes no acordo. A supervisão inclui mecanismos que garantem o cumprimento das regras a nível macro, tais como mecanismos comuns de revisão, e o cumprimento a nível micro, como a reparação individual.

56. Além destas três exigências de base, deverá ser prestada especial atenção às especificidades ligadas ao processamento de dados pessoais num contexto de aplicação da lei. Trata-se de facto de um domínio em que os direitos fundamentais podem sofrer restrições. Deverão portanto ser adoptadas garantias para compensar a restrição dos direitos individuais, especialmente no que diz respeito aos seguintes aspectos, atendendo ao seu impacto nas pessoas:

— Transparência: a informação e o acesso aos dados pessoais poderão ser limitados num contexto de aplicação da lei, devido por exemplo à discrição exigida por certas investigações. Enquanto na UE são tradicionalmente instituídos mecanismos adicionais para compensar esta limitação dos direitos fundamentais (que envolvem muitas vezes autoridades independentes de protecção de dados), deverá ser garantida a existência de mecanismos de compensação semelhantes uma vez transferida a informação para um país terceiro;

— Reparação: pelas razões atrás referidas, as pessoas deverão beneficiar de possibilidades alternativas de defender os seus direitos, em especial através de uma autoridade de supervisão independente e em tribunal;

— Conservação de dados: a justificação para o período de conservação dos dados poderá não ser transparente. Têm de ser tomadas medidas por forma a que tal não impeça o exercício efectivo dos direitos pelas pessoas em causa ou pelas autoridades de supervisão;

([20]) — Orientações das Nações Unidas sobre os dossiês relativos aos dados pessoais computorizados, adoptado pela Assembleia Geral em 14 de Dezembro de 1990, disponível em www.unhchr.ch/html/menu3/b/71.htm
— Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa, de 28 de Janeiro de 1981, disponível em www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— OCDE: Linhas de orientação sobre a protecção da privacidade e os fluxos transfronteiras de dados pessoais, adoptadas em 23 de Setembro de 1980, disponíveis em www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Decisão-Quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, disponível em http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, JO L 281 de 23.11.1995, p. 31.

([21]) Documento de trabalho de 24 de Julho de 1998 relativo às transferências de dados para países terceiros: Aplicação dos artigos 25.º e 26.º da Directiva da UE relativa à protecção dos dados; WP12.

— Responsabilização das autoridades de aplicação da lei: na falta de transparência efectiva, os mecanismos de controlo quer pelas pessoas quer pelas partes interessadas institucionais não podem de forma alguma ser exaustivos. Seria ainda assim essencial que tais controlos sejam firmemente estabelecidos, atendendo ao carácter sensível dos dados e às medidas coercivas que podem ser tomadas contra as pessoas com base no tratamento dos dados. A responsabilização é uma questão decisiva no que diz respeito aos mecanismos de controlo nacionais e igualmente às possibilidades de revisão pelo país ou região de origem dos dados. Tais mecanismos de revisão estão previstos em acordos específicos como o acordo PNR, e a AEPD recomenda vivamente a sua inclusão no instrumento geral.

V. **ANÁLISE DOS PRINCÍPIOS**

Introdução

57. Este capítulo analisa os 12 princípios incluídos no documento do Grupo de Contacto de Alto Nível segundo a seguinte perspectiva:

— Estes princípios mostram que os EUA e a UE têm alguns pontos de vista em comum sobre os princípios, podendo ser detectadas certas similitudes com os princípios da Convenção 108;

— No entanto, um acordo quanto ao nível dos princípios não é suficiente. Um instrumento jurídico deverá ser suficientemente forte para garantir o cumprimento;

— A AEPD lamenta que os princípios não sejam acompanhados de um memorando explicativo;

— Deveria ficar claro, antes de se entrar na descrição dos princípios, que ambas as partes têm o mesmo entendimento sobre a redacção utilizada, por exemplo no que diz respeito à noção de informação pessoal ou de pessoas protegidas. Neste contexto as definições são bem vindas.

1. Especificação do objectivo

58. O primeiro princípio enumerado no anexo do relatório do Grupo de Contacto de Alto Nível refere que a informação pessoal pode ser tratada para fins legítimos de aplicação da lei. Tal como atrás mencionado, isto diz respeito, no caso da União Europeia, à prevenção, detecção, investigação ou perseguição judicial de infracções penais. No entanto, no caso dos EUA, a interpretação da aplicação da lei vai além das infracções penais e inclui o controlo das fronteiras, a segurança pública e objectivos de segurança nacional. As consequências de tais discrepâncias entre os objectivos declarados pela UE e pelos EUA não são claras. Embora o relatório refira que na prática os objectivos podem coincidir em larga medida, continua a ser imperativo saber exactamente em que medida *não* coincidem. No domínio da aplicação da lei, tendo em conta o impacto das medidas tomadas sobre as pessoas, o princípio da limitação do objectivo tem de ser rigorosamente observado e os objectivos declarados têm de ser claros e circunscritos. Tendo em conta a reciprocidade prevista no relatório, a aproximação dos referidos objectivos parece igualmente essencial. Em resumo, é necessária uma clarificação da compreensão deste princípio.

2. Integridade/qualidade dos dados

59. A AEPD acolhe favoravelmente a disposição que prevê que a informação pessoal seja exacta, pertinente, atempada e completa, tal como necessário para um tratamento legal. Tal princípio é uma condição de base para um tratamento eficiente dos dados.

3. Necessidade/proporcionalidade

60. O princípio estabelece uma ligação clara entre a informação recolhida e a necessidade dessa informação para cumprir um objectivo de aplicação da lei juridicamente estabelecido. Esta exigência de uma base legislativa é um elemento positivo para avaliar a legitimidade do tratamento. A AEPD toma nota, no entanto, de que, embora isto reforce a certeza jurídica do tratamento, a base jurídica para esse tratamento consiste numa lei de um país terceiro. Uma lei de um país terceiro não pode, por si só, constituir uma base legítima para uma transferência de dados pessoais ([22]). No contexto do relatório do Grupo de Contacto de Alto Nível, parece assente que a legitimidade da lei de um país terceiro, por exemplo os Estados Unidos, é, em princípio, reconhecida. Deve ter-se presente que, se tal argumentação pode encontrar justificação neste caso atendendo a que os Estados Unidos são um Estado democrático, o mesmo regime não seria válido e não poderia ser transposto para as relações com qualquer outro país terceiro.

61. Qualquer transferência de dados pessoais tem de ser pertinente, necessária e adequada nos termos do anexo ao relatório do Grupo de Contacto de Alto Nível. A AEPD salienta que para ser proporcionado, o tratamento não pode ser indevidamente intrusivo, e as respectivas modalidades têm de ser equilibradas, tendo em conta os direitos e interesses das pessoas em causa.

62. Por esta razão, o acesso à informação deverá ter lugar numa base caso a caso, dependendo das necessidades práticas no contexto de uma investigação específica. O acesso permanente pelas autoridades de aplicação da lei do país terceiro a bases de dados situadas na UE seria considerado

([22]) Ver nomeadamente as alíneas c) e e) do artigo 7.º da Directiva 95/46/CE. No seu parecer 6/2002, de 24 de Outubro de 2002, sobre a transmissão da informação contida no manifesto de passageiros e outros dados pelas companhias aéreas aos Estados Unidos, o Grupo do Artigo 29.º declarou que não lhe parecia aceitável que uma decisão unilateral tomada por um país terceiro por razões do seu interesse público pudesse levar à transferência rotineira e por grosso de dados protegidos ao abrigo da directiva.

desproporcionado e sem justificação suficiente. A AEPD recorda que mesmo no contexto dos acordos existentes em matéria de intercâmbio de dados, por ex. no caso do acordo PNR, o intercâmbio de dados se baseia em circunstâncias específicas e é efectuado por um período limitado ([23]).

63. Segundo a mesma lógica, o período de conservação de dados deverá ser regulamentado: os dados deverão ser conservados tanto tempo quanto necessário, atendendo ao objectivo específico prosseguido. Se deixarem de ser pertinentes em relação ao objectivo identificado, deverão ser suprimidos. A AEPD opõe-se vivamente à constituição de armazéns de dados em que a informação sobre pessoas não suspeitas seja armazenada tendo em vista a sua eventual utilidade no futuro.

4. Segurança da informação

64. São desenvolvidos nos princípios medidas e procedimentos destinados a proteger os dados da utilização abusiva, alteração e outros riscos, havendo também uma disposição que limita o acesso a pessoas autorizadas. A AEPD considera satisfatórios estes aspectos.

65. Além disso, o princípio poderá ser complementado por uma disposição que preveja que deverão ser conservados registos das pessoas que têm acesso aos dados, o que reforçaria a eficácia das garantias no que diz respeito a limitar o acesso e a evitar a utilização abusiva dos dados.

66. Além disso, deverá ser prevista a informação mútua no caso de violação da segurança: caberá aos destinatários nos EUA bem como na UE informar os seus homólogos caso os dados recebidos tiverem sido alvo de divulgação ilícita. Tal contribuirá para aumentar a responsabilidade por um tratamento seguro dos dados.

5. Categorias especiais de informação pessoal

67. O princípio que proíbe o tratamento de dados sensíveis é, no entender da AEPD, consideravelmente enfraquecido pela excepção que permite todo e qualquer tratamento de dados sensíveis para os quais a legislação nacional preveja «garantias adequadas». Devido justamente ao carácter sensível dos dados, qualquer derrogação ao princípio da proibição deve ser justificada de forma adequada e precisa, sendo apresentada uma lista de objectivos e circunstâncias no âmbito dos quais um determinado tipo de dados sensíveis pode ser tratado, bem como uma indicação da qualidade dos controladores habilitados a tratar esse tipo de dados. Entre as garantias a adoptar, a AEPD considera que os dados sensíveis não deveriam constituir um elemento susceptível de desencadear uma investigação. Poderiam estar disponíveis em circunstâncias específicas mas apenas como informação adicional no que diz respeito à pessoa em causa já sob investigação. Estas garantias e condições devem ser enumeradas de forma limitativa no texto do princípio.

6. Responsabilização

68. Tal como desenvolvido nos pontos 55-56, a responsabilização das entidades públicas que tratam os dados pessoais tem de ser eficazmente garantida, e têm de ser dadas garantias no acordo sobre a forma como essa responsabilização se processará. Este aspecto reveste-se de grande importância, atendendo à falta de transparência tradicionalmente associada ao tratamento de dados pessoais num contexto de aplicação da lei. Nesta perspectiva, referir — como é o caso agora no anexo — que as entidades públicas deverão prestar contas sem dar qualquer explicação adicional sobre as modalidades e as consequências dessa prestação de contas não é uma garantia satisfatória. A AEPD recomenda que essa explicação seja dada no texto do instrumento.

7. Supervisão independente e eficaz

69. A AEPD apoia inteiramente a inclusão de uma disposição que preveja a supervisão independente e eficaz realizada por uma ou várias autoridades públicas de supervisão. Considera que se deve esclarecer de que modo se interpreta a independência, nomeadamente em relação a que entidades essas autoridades mantêm essa sua independência e perante que entidades são responsáveis. É necessário estabelecer critérios a este respeito, os quais deverão ter em conta a independência institucional e funcional em relação aos órgãos executivo e legislativo. A AEPD recorda que se trata de um elemento essencial para garantir a efectiva observância dos princípios acordados. As competências de intervenção e aplicação da lei dessas autoridades são igualmente determinantes tendo em conta a questão da responsabilização das entidades públicas que procedem ao tratamento de dados pessoais, tal como já se referiu mais acima. A sua existência e as competências de que estão investidas deverão ser claras para as pessoas a quem os dados dizem respeito, para que estas possam exercer os seus direitos, especialmente quando haja várias autoridades competentes, consoante o contexto do tratamento dos dados.

70. A AEPD recomenda, além disso, que qualquer futuro acordo preveja mecanismos de cooperação entre as autoridades de supervisão.

8. Acesso individual e rectificação

71. É necessário estabelecer garantias específicas no que toca ao acesso e à rectificação dos dados num contexto de aplicação da lei. Nesse sentido, a AEPD saúda o princípio segundo o qual devem ser facultados às pessoas interessadas o acesso e os meios necessários para obter a rectificação e/ou a eliminação das informações de carácter pessoal que lhes digam respeito. Todavia, subsiste alguma incerteza quanto à definição das pessoas em causa (todos devem

([23]) O presente acordo caduca e deixa de produzir efeitos sete anos após a data da sua assinatura, salvo se as partes decidirem de comum acordo substitui-lo.

gozar de protecção e não só os cidadãos do país em questão), bem como relativamente às condições em que as pessoas em causa podem levantar objecções ao tratamento das informações que lhes digam respeito. Importa igualmente precisar quais os «casos adequados» em que são ou não admissíveis objecções. Não deve restar para as pessoas em causa nenhuma dúvida quanto às circunstâncias — consoante, por exemplo, o tipo de autoridade, o tipo de investigação ou outros critérios — em que podem exercer os seus direitos.

72. Além disso, não havendo uma possibilidade directa de levantar objecção ao tratamento dos dados por motivos justificados, deverá estar disponível outra possibilidade indirecta de verificação, através da autoridade independente responsável pela supervisão do tratamento dos dados.

9. Transparência e informação

73. A AEPD salienta uma vez mais a importância de uma efectiva transparência, para que as pessoas em causa possam exercer os seus direitos e para contribuir para a responsabilização geral das autoridades públicas que procedem ao tratamento de dados pessoais. A AEPD apoia os princípios definidos e insiste, em especial, na necessidade de as informações serem fornecidas *tanto* a título geral *como* a título individual, directamente às pessoas em causa, o que se encontra reflectido no princípio definido no ponto 9 do anexo.

74. No entanto, no Capítulo 2, A. B. (Princípios acordados) o relatório refere que, nos EUA, a transparência pode implicar a publicação, individualmente ou em conjunto, no Registo Federal, da informação fornecida a título individual e a sua divulgação em processo judicial. Não deve restar dúvida de que a publicação num jornal oficial não é, por si só, suficiente para assegurar a informação adequada das pessoas em causa. Para além da necessidade de se proceder à informação a título individual, a AEPD recorda que a informação deve ser apresentada de uma forma e numa linguagem facilmente inteligíveis para a pessoa em causa.

10. Reparação

75. A fim de garantir o efectivo exercício dos seus direitos, as pessoas interessadas devem ter a possibilidade de apresentar queixa perante uma autoridade independente de protecção de dados, bem como de recorrerem para um tribunal independente e imparcial. Ambas estas vias de recurso deverão ser igualmente acessíveis.

76. É necessário assegurar o acesso a uma autoridade independente de protecção de dados, uma vez que esta fornece uma assistência flexível e menos onerosa num contexto — da aplicação da lei — que pode ser bastante opaco para o cidadão comum. As autoridades de protecção de dados podem também prestar assistência no exercício de direitos de acesso em nome da pessoa interessada, quando circunstâncias excepcionais vedem a esta última o acesso directo aos dados que lhe dizem respeito.

77. O acesso ao sistema judiciário constitui uma outra garantia indispensável de que as pessoas em causa podem recorrer para uma autoridade que se insere num ramo do sistema democrático distinto do das instituições públicas que procedem efectivamente ao tratamento dos dados que lhes dizem respeito. O Tribunal Europeu de Justiça ([24]) considerou este tipo de recurso efectivo junto de um tribunal como sendo «essencial para garantir ao particular a protecção efectiva do seu direito. […] Constitui um princípio geral do direito comunitário, que decorre das tradições constitucionais comuns dos Estados-Membros e que teve a sua consagração nos artigos 6.º e 13.º da Convenção Europeia dos Direitos do Homem.». A existência de um recurso judicial encontra-se igualmente prevista no artigo 47.º da Carta dos Direitos Fundamentais da União Europeia e no artigo 22.º da Directiva 95/46/CE, sem prejuízo de quaisquer recursos administrativos.

11. Decisões individuais automatizadas

78. A AEPD saúda a disposição que prevê salvaguardas adequadas em caso de tratamento automatizado de dados pessoais. A AEPD regista que as condições de aplicação deste princípio seriam esclarecidas mediante um entendimento comum do que é considerado uma acção adversa significativa contra os interesses relevantes de um particular.

12. Transferências para outros países

79. Nalguns casos, não estão bem esclarecidas as condições a que devem obedecer as transferências de informação para outros países. Em especial, quando a transferência deve obedecer às disposições de acordos e convénios internacionais entre o país emissor e o país receptor, dever-se-ia especificar se se trata de acordos entre os dois países que efectuaram a primeira transferência ou entre os dois países envolvidos na transferência em questão. No entender da AEPD, será sempre necessário um acordo entre os dois países que procedem à primeira transferência.

80. A AEPD regista também uma definição muito ampla dos legítimos interesses públicos que justificam a transferência. Há falta de clareza quanto à segurança pública, parecendo também injustificada e excessiva, num contexto de execução da lei, a extensão das transferências em caso de atentado contra a ética ou as profissões regulamentadas.

VI. **CONCLUSÃO**

81. A AEPD saúda o trabalho conjunto levado a cabo pelas autoridades da UE e dos EUA no domínio da aplicação da lei, em que a protecção de dados é fundamental. No entanto, a AEPD insiste em que se trata de uma questão complexa, em especial no que diz respeito à precisão do respectivo âmbito e natureza, pelo que merece uma análise cuidadosa e aprofundada. Deverá ser cuidadosamente

([24]) Processo 22/84 *Johnston* [1986], Colect., p. 1651; Processo 222/86 *Heylens* [1987], Colect., p. 4097; Processo C-97/91 *Borelli* [1992] Colect., p. I-6313.

apreciado o impacto de um instrumento transatlântico em matéria de protecção de dados tanto para os cidadãos como relativamente ao quadro jurídico actualmente em vigor.

82. A AEPD exige maior clareza e disposições concretas, especialmente no que toca aos seguintes aspectos:

— Clarificação da natureza do instrumento, que deveria ser juridicamente vinculativo para assegurar suficiente certeza jurídica;

— Uma minuciosa averiguação da adequação, com base nos requisitos essenciais em matéria de conteúdo e especificidade do regime e quanto aos seus aspectos que se prendem com a supervisão. A AEPD considera que apenas se poderá reconhecer a adequação do instrumento geral se combinada com acordos específicos numa base caso a caso;

— Um âmbito de aplicação bem delimitado, acompanhado de uma clara definição comum dos objectivos da aplicação da lei;

— Precisão das modalidades da eventual participação de entidades privadas nas transferências de dados;

— Observância do princípio da proporcionalidade, o que implica que o intercâmbio de dados se faça caso a caso, a partir de uma necessidade concreta;

— Existência de mecanismos eficazes de supervisão e de possibilidades de recurso para as pessoas em causa, nomeadamente o recurso judicial e administrativo;

— Medidas eficazes que garantam a todas as pessoas em causa o exercício dos respectivos direitos, independentemente da sua nacionalidade;

— Participação de autoridades independentes em matéria de protecção de dados, especialmente no que diz respeito à supervisão e à assistência às pessoas interessadas.

83. A AEPD insiste na necessidade de evitar qualquer precipitação ao definir os princípios, o que só poderia conduzir a soluções pouco satisfatórias e a um efeito contraproducente em termos de protecção de dados. A melhor maneira de avançar seria pois desenvolver um roteiro com vista a um possível acordo numa fase posterior.

84. A AEPD exige também maior transparência para o processo de definição dos princípios da protecção de dados. Só com a participação de todas as partes interessadas, nomeadamente o Parlamento Europeu, poderá este instrumento granjear, através de um debate democrático, o necessário apoio e reconhecimento.

Feito em Bruxelas, em 11 de Novembro de 2008.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados